EXHIBIT 5

16 MAG 8347

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All Content and Other Information Associated with the Email Accounts: btcooney@gmail.com, darcher@rosemontseneca.com and smomtazi@rosemontseneca.com Maintained at Premises Controlled by Google; and darcher@rosemontcapital.com and smomtazi@rosemontcapital.com Maintained at Premises Controlled by Apptix, USAO Reference No. 2015R01447

SEARCH WARRANT

TO: Google ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Shannon Bieniek of the FBI, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts btcooney@gmail.com, darcher@rosemontseneca.com, and smomtazi@rosemontseneca.com maintained at premises controlled by Google, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance.

The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

Dated: New York, New York

12/28/16 4:20 p.m.

Date Issued Time Issued

S/Barbara Moses

UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Barbara Moses
United States Magistrate Judge
Southern District of New York

Email Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Google (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts btcooney@gmail.com, darcher@rosemontseneca.com, and smomtazi@rosemontseneca.com (the "Subject Accounts").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts from January 1, 2014 to May 11, 2016:

i. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Provider's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Provider's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for a certain period of time.[3]

---

[3] Emails and attachments stored by a subscriber on a server maintained by the Provider may not necessarily be located on the subscriber's home computer. The subscriber may store emails or

ii. *Google Docs, Sheets, and Slides.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs," "Google Sheets," and "Google Slides." Users can use Google Docs, Sheets, and Slides to create online documents that can be stored on or saved to the user's Google Drive.

iii. *Google Drive content.* Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

iv. *Google Chats and Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

---

other files on that Provider's servers for which there is insufficient storage space in the subscriber's computer or which the subscriber does not wish to maintain on that computer. Additionally, a Provider may have kept emails or other files pursuant to a preservation letter even though the subscriber has deleted the emails or files. A search of the files in the computer in the subscriber's residence would therefore not necessarily uncover the files that the subscriber has stored on the Provider's servers.

v. *Address book.* The Provider also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

vi. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and other email addresses associated with the account. Specifically, with regard to other email addresses associated with the account, Google maintains records regarding (1) recovery and (2) alternate email accounts, which can be used to sign in to the account and recover a password; (3) fetching and (4) forwarding addresses, which are email accounts from which the primary account receives emails and forwards emails, respectively; (5) domain aliases or (6) separate domains associated with the account, which are means by which accounts with other domain names can be associated with a primary account; (7) other Google accounts that have access to the primary account, which access can be granted by the user of the primary account; and (8) other email accounts that are associated with the primary account. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

vii. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

viii. *Customer correspondence.* The Provider also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

ix. *Location data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

x. *Picasa Web Albums.* Google provides users with a certain amount of free storage, currently 1 gigabyte, through a service called "Picasa Web Albums" that allow for users to store and share digital photographs. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Picasa Web Albums. This metadata includes what is known as exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

xi. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile equipment Identifier), device ID, and/or serial number of the devices. Each of those identifiers uniquely

identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

xii. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google's proprietary web browser, as well as other Google applications.

xiii. *Google Alerts.* Google provides a service that allows for email notifications any time Google finds new results on a topic of interest to a particular user. Users can create an alert by entering keywords for which they would like to receive email notifications. Once an alert is set up, Google will send emails to the designated email account every time Google finds new search results for the keywords entered by the user.

xiv. *Google Webmaster Tools and Google Search Console.* Google provides a service (previously called Webmaster Tools but renamed Google Search Console as of May 20, 2015) that allows users to monitor and maintain their site's presence in Google Search results. The tool allows a user to ensure that Google can access the content of a website; submit new content for purposes of crawling (i.e., to ensure that Google captures data from the website for purposes of its search engine) and remove content that the user does not want shown in each result; create and monitor content; see what queries caused a site to appear in search results, and the amount of traffic generated by such searches, and what websites are linked to that site; and other activity.

xv. *Google Analytics.* Google Analytics is a subscription service offered by Google, which caters to online businesses. A business subscribed to Google Analytics can use the serve to monitor traffic to and within the business's website. Google Analytics collects information about a website's users by installing a "cookie"—or a small piece of data—on the computer of each user of the business's website, which then collects information about the user's interactions with the website by, for example, tracking what pages of the business's website the

user visits. Among the user data collected by Google Analytics is "referral traffic," which lets the business see what websites are referring traffic to the business's website—that is, the websites that users are visiting immediately before visiting the subscriber's website. Such data can help the subscriber to understand the sources of its online business. Google Analytics provides a platform through which subscriber can run various queries and generate various reports based on the website traffic data collected through the service. Google Analytics retains records of the queries run and reports generated by the subscriber.

xvi. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xvii. *Google Apps and Google Apps Administrator Control Panel.* Google Apps is a package of cloud-based services that allow for an organization to communicate in ways beyond emailing and chatting—such as through video conferences, social media, real-time document collaboration, and other things. A user can sign up for Google Apps by providing a domain name that s/he wishes to use with Google services. Google then allows for a group of people to use Gmail, Calendar, Drive, and other services together. The Google Apps Administrator Panel allows a designated user to serve as the administrator of an organization's Google Apps account, allowing the administrator to control access to mail, data, and security for others in the organization. Google Apps Administrator Control Panel lets an administrator monitor how individual services are being used, as well as managing individual domains.

xviii. *Google URL Shortener.* Google provides a service that allows a user to shorten URLs to make them easier to share, and tracks the clicks that a shortened URL receives.

xix. *Preserved and backup records*. The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1348, and Title 15, United States Code, Sections 78j(b) and 78ff, Title 17, Code of Federal Regulations, Sections 240.10b-5; conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371; investment advisor fraud, in violation of Title 15, United States Code, Sections 80b-6 and 80b-17; and conspiracy to commit investment adviser fraud, in violation of Title 18, United States Code, Section 371, among other statutes, including the following:

- evidence of the agreement to engage in a fraudulent scheme involving the issuance of bonds on behalf of the Wakpamni Lake Community Corporation ("WLCC") and the misappropriation of the proceeds of those bonds, from January 1, 2014 to May 11, 2016;
- evidence of communications and/or meetings involving or related to the bonds issued on behalf of the WLCC, including but not limited to:

- all emails with or pertaining to Jason Galanis, John Galanis, Gary Hirst, Hugh Dunkerley, Michelle Morton, Devon Archer, and Bevan Cooney;
- all emails with or pertaining to entities involved in the issuance, placement, purchase or sale of the bonds;
- all emails with or pertaining to entities involved in the receipt and/or use of the bond proceeds;

- evidence of crime (*e.g.*, agreement to engage in unlawful conduct, references to or discussion of unlawful conduct), communications constituting crime (*e.g.*, emails containing fraudulent representations); and identities and locations of co-conspirators or victims (communications with co-conspirators or victims, photos or other attachments, address book information).
- e-mail communications with co-conspirators;
- e-mails that can be helpful to establish user identity;
- email header information which can assist in placing the targets or confederates at a certain time and place;
- geographic location of user, computer, or device (*e.g.*, the content and header information can both indicate that the email was communicated through a particular physical location; metadata from photo attachments can reflect geographic location);
- identities and locations of co-conspirators or victims (communications with co-conspirators, photos or other attachments, address book information);
- location of other evidence (*e.g.*, emails reflecting registration of other online accounts potentially containing relevant evidence);

- passwords or other information needed to access the user's computer or other online accounts.

16 MAG 8347

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All Content and Other Information Associated with the Email Accounts: btcooney@gmail.com, darcher@rosemontseneca.com and smomtazi@rosemontseneca.com Maintained at Premises Controlled by Google; and darcher@rosemontcapital.com and smomtazi@rosemontcapital.com Maintained at Premises Controlled by Apptix, USAO Reference No. 2015R01447

SEARCH WARRANT

TO: Apptix ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Shannon Bieniek of the FBI, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts darcher@rosemontcapital.com and smomtazi@rosemontcapital.com maintained at premises controlled by Apptix, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance.

The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

Dated: New York, New York

12/28/16 4:20 pm

Date Issued Time Issued

S/Barbara Moses

UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Barbara Moses
United States Magistrate Judge
Southern District of New York

Email Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Apptix (the "Provider"), headquartered at 13461 Sunrise Valley Drive, Ste 300, Herndon, VA 20171, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts darcher@rosemontcapital.com and smomtazi@rosemontcapital.com (the "Subject Accounts").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts from January 1, 2014 to May 11, 2016:

i. Email contents. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Providers' servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Providers' computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Providers' servers for a certain period of time.[4]

[4] Emails and attachments stored by a subscriber on a server maintained by the Provider may not necessarily be located on the subscriber's home computer. The subscriber may store emails or other files on that Provider's servers for which there is insufficient storage space in the subscriber's computer or which the subscriber does not wish to maintain on that computer. Additionally, a

ii. Address book. The Providers also allow subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. Subscriber and billing information. The Providers collect and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Providers also maintain records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the Providers maintain records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. Transactional information. The Providers also typically retain certain transactional information about the use of each account on its system. This information can include records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through the Providers' websites).

v. Customer correspondence. The Providers also typically maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. Preserved records. The Providers also maintain preserved copies of the foregoing categories of records with respect to an account, typically for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

Provider may have kept emails or other files pursuant to a preservation letter even though the subscriber has deleted the emails or files. A search of the files in the computer in the subscriber's residence would therefore not necessarily uncover the files that the subscriber has stored on the Provider's servers.

III.Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1348, and Title 15, United States Code, Sections 78j(b) and 78ff, Title 17, Code of Federal Regulations, Sections 240.10b-5; conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371; investment advisor fraud, in violation of Title 15, United States Code, Sections 80b-6 and 80b-17; and conspiracy to commit investment adviser fraud, in violation of Title 18, United States Code, Section 371, among other statutes, including the following:

- evidence of the agreement to engage in a fraudulent scheme involving the issuance of bonds on behalf of the Wakpamni Lake Community Corporation ("WLCC") and the misappropriation of the proceeds of those bonds, from January 1, 2014 to May 11, 2016;
- evidence of communications and/or meetings involving or related to the bonds issued on behalf of the WLCC, including but not limited to:
    - all emails with or pertaining to Jason Galanis, John Galanis, Gary Hirst, Hugh Dunkerley, Michelle Morton, Devon Archer, and Bevan Cooney;
    - all emails with or pertaining to entities involved in the issuance, placement, purchase or sale of the bonds;
    - all emails with or pertaining to entities involved in the receipt and/or use of the bond proceeds;

- evidence of crime (*e.g.*, agreement to engage in unlawful conduct, references to or discussion of unlawful conduct), communications constituting crime (*e.g.*, emails containing fraudulent representations); and identities and locations of co-conspirators or victims (communications with co-conspirators or victims, photos or other attachments, address book information).
- e-mail communications with co-conspirators;
- e-mails that can be helpful to establish user identity;
- email header information which can assist in placing the targets or confederates at a certain time and place;
- geographic location of user, computer, or device (*e.g.*, the content and header information can both indicate that the email was communicated through a particular physical location; metadata from photo attachments can reflect geographic location);
- identities and locations of co-conspirators or victims (communications with co-conspirators, photos or other attachments, address book information);
- location of other evidence (*e.g.*, emails reflecting registration of other online accounts potentially containing relevant evidence);
- passwords or other information needed to access the user's computer or other online accounts.